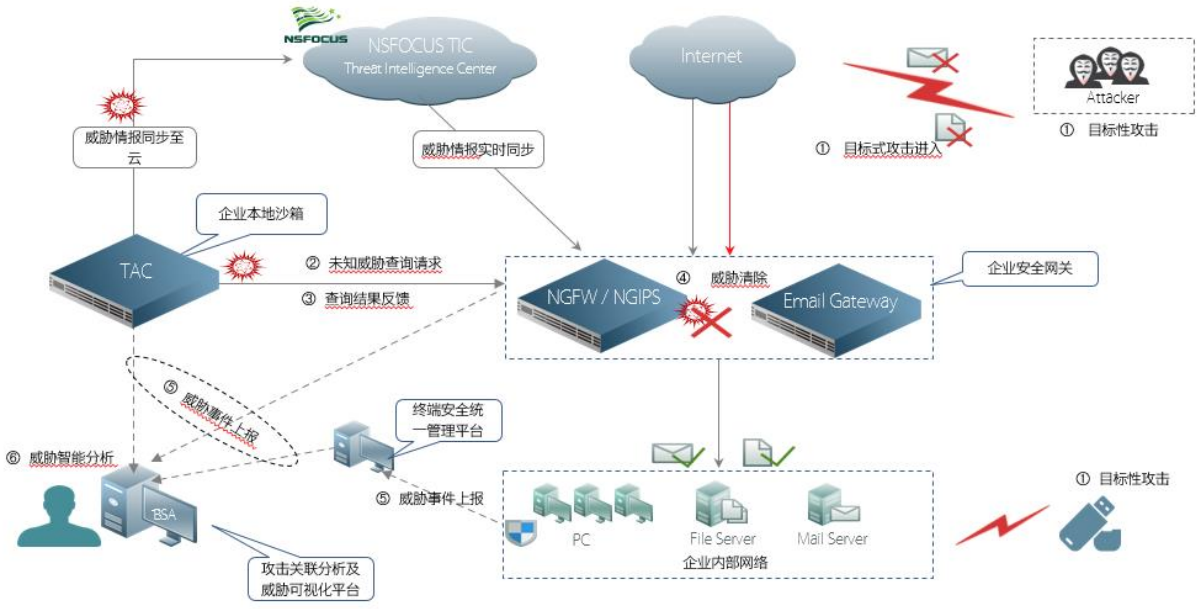
防护方案

Hacking Team 数据泄露



Content

攻击：谁在攻击？ 3

Hacking Team 及 Gamma Group 3
泄露数据 4
影响程度 4

防护思路 5

Detect 6
Deny 7

解决方案 8

应对 0Day 8
方案优势 9

威胁情报 10

关于绿盟科技 10

内容导读

7 月 5 日晚，一家意大利远程控制软件厂商 Hacking Team 的内部数据被泄露出来，其影响力不亚于斯洛登事件及维基解密事件，绿盟科技威胁响应中心随即启动应急响应工作。

1. 6 日，威胁响应中心启动应急分析工作，绿盟 TAC 产品拦截到 Flash 0Day 漏洞攻击；
2. 6 日夜，相关信息及初步建议，第一时间告知客户关注；
3. 7 日，在官网网站发布紧急通告，建议广大用户关注事件进展。分析工作进展进展中；
4. 9 日，发布 Hacking Team 远程控制系统简要分析报告，同时发布防护方案；

本报告从此次事件中获取的样本入手，分析其包含的数据及影响，为用户思考下一步的应对方案，给出了防护思路及解决方案。

在看完本报告后，如果您有不同的见解，或者需要了解更多信息，请联系：

- 绿盟科技威胁响应中心微博
- http://weibo.com/threatresponse
- 绿盟科技微博
- http://weibo.com/nsfocus
- 绿盟科技微信号
- 搜索公众号 绿盟科技

攻击：谁在攻击?

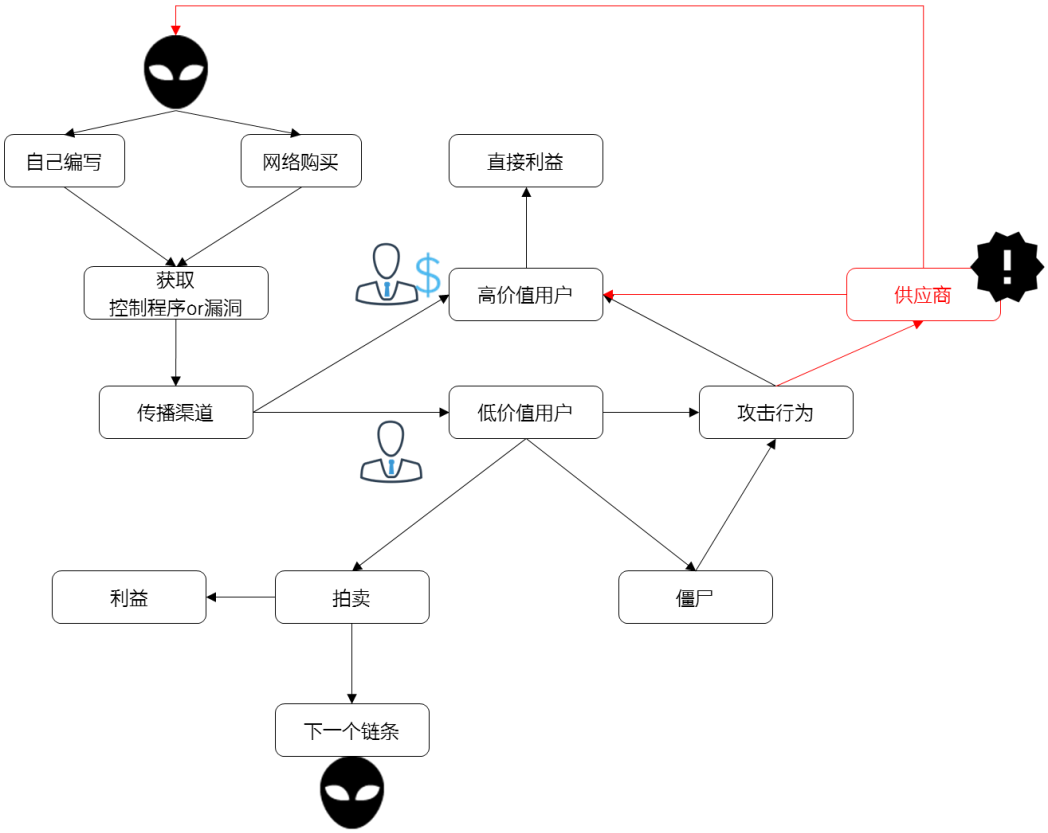
7 月 5 日晚，一家意大利软件厂商[①]被攻击，其掌握的 400GB 数据泄露出来，由此可能引发的动荡，引起了业界一片哗然。截止发稿时止，有多个组织声称对此行为负责，包括 Gamma Group Hacker[②]。虽然目前没有事实表明该声称确实可信，但由此让黑色产业链条中的一种“新”形态暴露出来，即从攻击最终用户演变为攻击中间链条乃至攻击者组织之间的互相厮杀，这种形态已经从黑产上升到供应商、政府机构之间的问题，这不得不说，对涉及中间链条的组织，敲响了警钟。

Hacking Team 及 Gamma Group

Hacking Team 在意大利米兰注册了一家软件公司，主要向各国政府及法律机构销售入侵及监视功能的软件。其远程控制系统可以监测互联网用户的通讯、解密用户的加密文件及电子邮件，记录 Skype 及其他 VoIP 通信，也可以远程激活用户的麦克风及摄像头。其总部在意大利，雇员 40 多人，并在安纳波利斯和新加坡拥有分支机构，其产品在几十个国家使用[③]

无独有偶，这次声称对此次事件负责的组织，Gamma Group International[④]也曾经在 2014 年的 8 月被人入侵过，在那次的事件中，该组织被泄露了 40GB 的内部文档和恶意程序代码。这个组织无论从背景还是业务都与 Hacking Team 类似，但是一家英国的公司。

地下产业链各方的相互厮杀由此可见一斑，这里简单用一张图来简单展示一下其中的一个部分。值得关注的是，这次通过攻击供应商等中间链条获得攻击数据的动态。



图注：黑色产业链

① Hacking Team 主页, http://www.hackingteam.it/
② Gamma Group Hacker, http://www.ibtimes.co.uk/who-hacked-hacking-team-gamma-group-hacker-holds-their-hand-1509662
③ Hacking Team介绍 https://en.wikipedia.org/wiki/Hacking_Team
④ Gamma Group 主页, https://www.gammagroup.com/

泄露数据

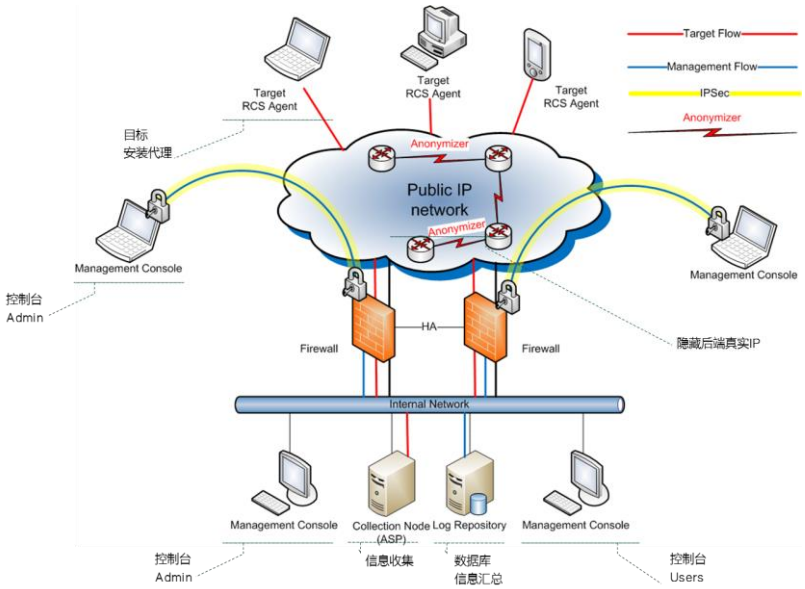
此次事件中泄露的数据多达 400GB，数据包中主要包含几个大的部分：

- 远程控制软件源码，也是其核心，暂且称之为 Hacking Team RCS（Remote Control System）
- 反查杀分析工具及相关讨论文档
- 0Day、漏洞及相关入侵工具
- 入侵项目相关信息，包括账户密码、数据及音像资料
- 办公文档、邮件及图片
- 其他

影响程度

在这些数据中，绿色标注的 3 类比较引人关注，这 3 类数据将对各个不同的领域造成影响

- 更频繁：0Day、漏洞及相关入侵工具，从目前获取的信息来看
  - Flash 相关的应用及软件使用量非常庞大，Windows 平台上几乎是所有的用户都会用到；
  - 这些漏洞的流入黑色产业链，会让攻击更加快速和复杂化
- 门槛低：Hacking Team RCS，是该组织主要输出的软件，从目前获取的信息来看[①]
  - 可以获取目标用户的电话、电脑的全部信息及影音资料；
  - 涉及的桌面 OS 从 Windows 到 MacOs X，手机 OS 基本覆盖了市场上流行的系统；
  - 受该工具及其已经感染的客户端数量的影响，会让攻击门槛降低
- 影响大：入侵项目相关信息，这里面包含了各种入侵过程资料，甚至包含了已经成功获取的账户密码及相关资料，一旦被恶意攻击者获取并利用，将会在黑色产业链中进一步发酵。



图注：Hacking Team 远程控制系统

① Hacking Team RCS 分析，《简要分析：Hacking Team 远程控制系统》

防护思路

绿盟科技威胁响应中心在长年对黑客组织事件的追踪及分析中，获得了丰富的经验积累，借鉴及建立了一些模型去理解它们，试图从中找到规律，以便为应对未来的未知威胁提供经验借鉴。针对此次事件，这里使用 Intrusion Kill Chain 模型跟大家进行探讨，虽然不一定适合所有业务环境，但希望可以帮助大家找到指定自身防护方案的一点灵感。

Intrusion Kill Chain 模型[①]精髓在于明确提出网络攻防过程中攻防双方互有优势，防守方若能阻断/瓦解攻击方的进攻组织环节，即是成功地挫败对手的攻击企图。模型是将攻击者的攻击过程分解为如下七个步骤：Reconnaissance（踩点）、Weaponization（组装）、Delivery（投送）、Exploitation（攻击）、Installation（植入）、C2（控制）、Actions on Objectives（收割），如下图：

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

通过目前对 Hacking Team RCS 软件的分析情况来看，主要通过如下三种方式入侵目标：

- 感染移动介质　　与很多木马、病毒及流氓软件的传播方式一样，该软件首先还是采取这种低成本的方式进行，感染一些能够接触目标的移动媒体，比如 CD-ROM、USB 等，即便是 OS 或者 BIOS 设置了密码也一样可以感染，从而获取一些环境数据，比如电脑是否可以上网等，为后续的动作提供参考依据。
- 代理攻击　　采用软件或硬件的系统，能够在网络会话过程中修改和注入数据，在某些情况下，可以注入到系统并难以被检测到。同时，也能够感染 Windows 平台上的可执行文件，如果目标电脑从网站上下载并执行这些可执行文件时，Agent 将在后台自动安装，用户不会知晓。
- APT　　如上两种方式都无法奏效的时候，就会采用多种形式组合入侵，采用相关的漏洞、入侵工具及更多利用手段。

针对这些入侵方式，下面来分阶段讨论防护思路。

[①] Intrusion Kill Chain（或称为 Cyber Kill Chain）模型由 Lock Martin 公司 Eric M. Hutchins 等三位安全研究员在 2011 年 3 月举行的 ICIW 大会 上公布。

Detect

在这个阶段，建议您将当前 IT 环境中的漏洞扫描系统升级到最新版本后，尽快开始对业务系统进行扫描，尤其是受此次 Flash 0Day 漏洞影响的业务系统平台进行一次完整的漏洞扫描。

此次事件中，绿盟威胁分析系统[①]（NSFOCUS Threat Analyze Center，TAC）即体现出优越性，即通过独创的静态检测和动态检测引擎，能够不依赖于攻击特征识别恶意软件及其危害程度，率先侦测到 Flash 0Day 漏洞。

绿盟 TAC 可有效检测通过网页、电子邮件或其他在线文件共享方式进入网络的已知和未知恶意软件，发现利用 0day 漏洞的 APT 攻击行为，保护客户网络免遭利用 0day 漏洞等攻击造成的各种风险，如敏感信息泄露、基础设施破坏等。

NSFOCUS

详情检测报告

生成时间：2015-07-07 17:17:52

基本信息

威胁等级	高威胁		
用户		时间	2015-07-07 14:40:45
客户端IP	192.168.7.139	客户端端口	9651
服务端IP	104.20.16.176	服务端端口	80
应用	HTTP下载	协议	TCP
域名	ht.transparencytoolkit.org	URL	/gitlab/Release-Edn/2015-009-Windows-Multi-Browser.zip
来源	http://ht.transparencytoolkit.org/gitlab/Release-Edn/		
相对路径	2015-009-Windows-Multi-Browser.zip\resources\ie_template.swf	父文件名	2015-009-Windows-Multi-Browser.zip
文件名	ie_template.swf	类型	SWF

分析总结

静态检测

AS引擎检测到Shellcode特征

```
E8 00 00 00 00          call    0x5
58                      pop     eax
25 00 F0 FF FF          and     eax,0xfffff000
E8 00 00 00 00          call    0x10
5E                      pop     esi
90                      nop
BB 11 BA 11 BA          mov     ebx,0xba11ba11
3B 1E                   cmp     ebx,[esi]
74 03                   jz      0x1e
4E                      dec     esi
EB F4                   jmp     0x12
8B 09                   mov     ecx,[ecx]
51                      push    ecx
56                      push    esi
```

绿盟 TAC 能够在如下两个阶段对此次事件所带来的可能攻击进行检测

- Delivery 阶段：发现（detect）试图传输到内网的恶意软件（文件），包括已知和未知的高级恶意软件；
- Installation 阶段：发现高级恶意软件成功利用后，试图从控制端下载更多恶意程序。

[①] 绿盟威胁分析系统 TAC，http://www.nsfocus.com.cn/products/details_22_1.html

Deny

如果您已经部署了绿盟网络入侵防护系统(Network Intrusion Prevention System，简称 NIPS[①])，在升级最新的升级包后，即可阻断 Flash 0Day 漏洞所带来的攻击，并持续获得敏感数据保护、客户端防护、服务器非法外联防护、僵尸网络防护等多项防护。

请所有使用绿盟产品的用户尽快升级。绿盟科技已在软件升级公告中提供规则升级包，规则可以通过产品界面的在线升级进行。如果您的业务系统暂时还无法升级规则包，那么可以在软件升级页面中，找到对应的产品，通过下载升级包，以离线方式进行升级。 相关信息请访问产品升级公告 http://update.nsfocus.com/

另外，用户如果已部署绿盟 NIPS 产品，可以通过增加 TAC 防护组件的方式，使企业本地网络具备未知威胁发现能力，并与绿盟 NIPS 形成联动，在第一时间做到未知威胁检测、拦截。

Patch

在这个阶段，建议您尽快的安装就此次泄露出来的资料库中所包含的 Flash 0Day 漏洞，Adobe 官方已经修复了漏洞，并提供了升级版本，请广大用户尽快升级到最新版本。FLASH 更新步骤如下：

- 打开 https://get.adobe.com/flashplayer/?loc=cn
- 点击立即安装，保存安装包，下载完成后执行安装文件

0Day 漏洞一旦被公开，往往也是被攻击者利用最为猖狂的时候。在此，安全专家建议：

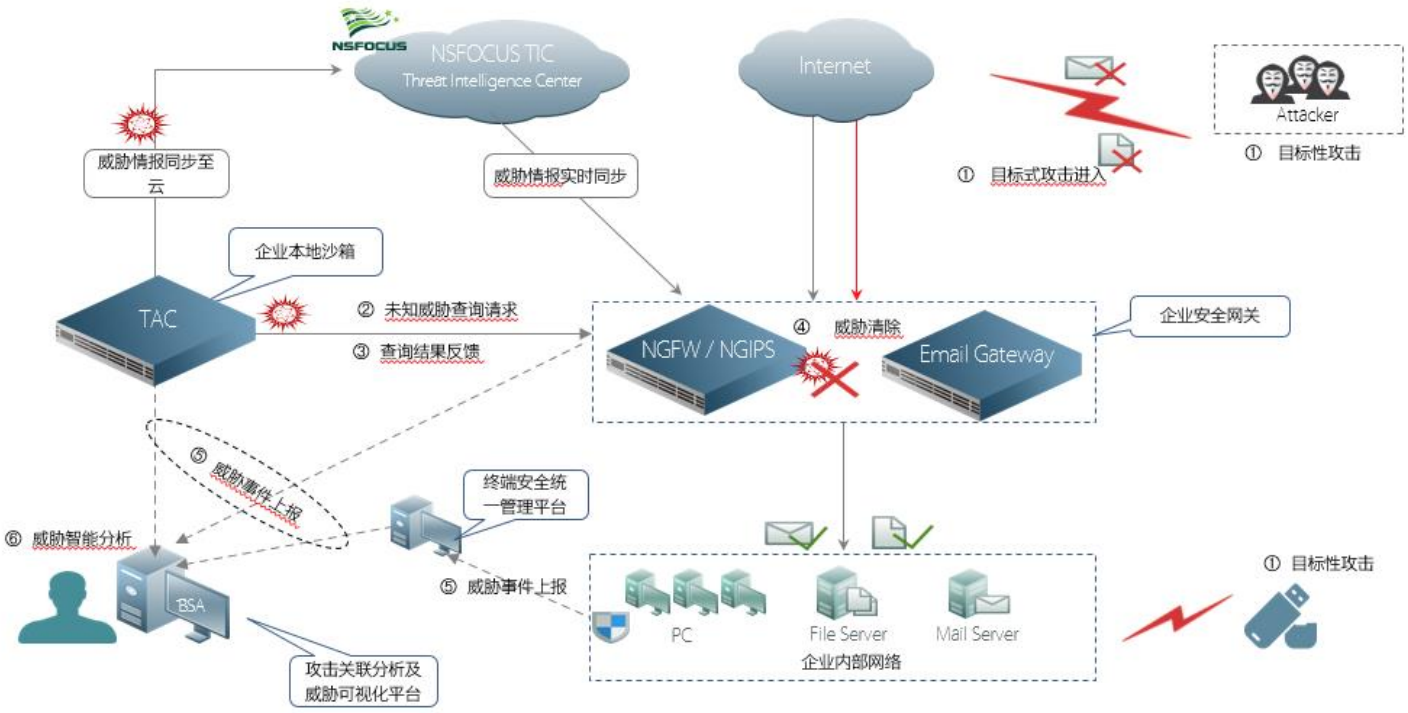
- 安装反病毒软件进行全盘查杀，并第一时间更新系统和 Flash 补丁
- 推荐使用安全级别更高的猎豹，FireFox 浏览器
  - ·Chrome 用户请升级至最新版本(>=43)
  - ·IE，Chrome 用户请手动升级 Flash 至最新版本
- 养成良好的上网习惯和安全意识，
  - ·提高内部员工的安全意识和建立完备的监控体系是防范 APT 的重要手段。
  - ·建议对内部员工开展广泛的安全意识培训，避免出现使用弱口令、点击不明来历邮件附件、访问恶意网站等危险行为。不随意打开陌生人通过 QQ 等发送的网页链接，不随意打开垃圾邮件

[①] 绿盟网络入侵防护系统 NIPS，http://www.nsfocus.com.cn/products/details_22_3.html

解决方案

绿盟下一代威胁解决方案（NGTP 解决解决方案），是针对 APT 威胁进行检测和防御的解决方案。NGTP 解决方案聚焦 APT 攻击链条，检测和防御 APT 攻击链中攻击，潜伏和盗取三个主要环节。重点检测和防御在攻击尝试阶段，进入后的潜伏和扩展攻击阶段，以及最终盗取数据目的阶段。

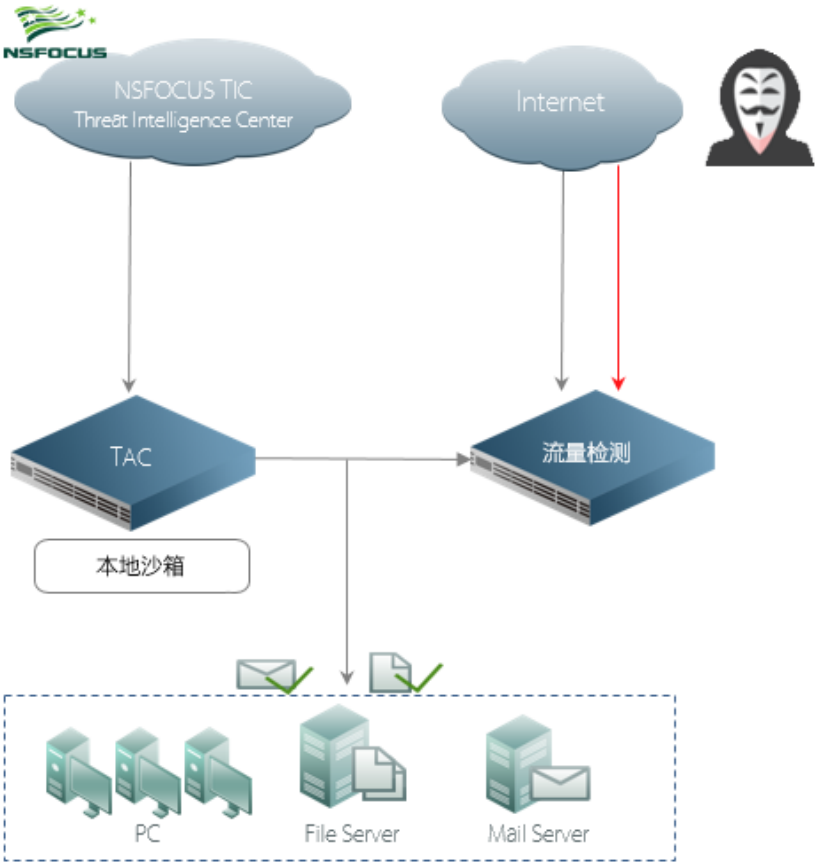
NGTP 解决方案以全球威胁情报云为纽带，以未知威胁检测为核心，通过与传统终端、网关设备联动，实现跨厂商的威胁情报的共享，以及企业威胁态势可视化，最终达到提升企业 APT 威胁防护的能力的目标。



应对 0Day

NGTP 针对 0Day 漏洞攻击的解决方案，由本地沙箱 TAC，威胁防御模块 IPS，绿盟安全信誉和 ESPC 管理等系统构成。NGTP 方案防御 0Day 漏洞攻击的流程：

- 第一步：要经过本地沙箱系统 TAC 的检测，TAC 提供静态检测引擎和虚拟执行引擎，对恶意软件进行 Shellcode 静态分析，然后再进行虚拟执行。通过这两步分析，从 Hacking Team 组织泄露的 0Day 攻击软件被识别出来；
- 第二步：TAC 检测出恶意软件的来源，生成信誉信息，包括文件的信誉和攻击源 IP 等信息，同步到本地的安全管理中心 ESPC，形成本地的信誉库；
- 第三步：NIPS 从本地信誉库接收到恶意软件的信誉信息，对发起攻击的源 IP 实现阻断，并生成告警日志。



方案优势

- APT 威胁检测和防御的全面性　　绿盟下一代威胁解决方案，能够全面的对 APT 威胁检测和防御。无论是网络，Web 还是邮件，终端众多通道，都是 APT 威胁可能利用的通道，NGTP 解决方案，不仅在网络边界进检测和防御，还在企业内网，邮件服务器，终端等多个层面进行检测和防御。既能够实时进行检测和阻断，还利用大数据分析平台，进行事后的分析和调查。
- APT 检测的准确性　　绿盟下一代威胁解决方案，利用本地沙箱和云端安全信誉，准确地对 APT 威胁检测和防御。本地沙箱提供了恶意软件静态检测和虚拟执行手段，检查恶意软件 Shellcode，并且模拟真实的 PC 环境进行验证，极大提高恶意软件的准确性；同时，云端信誉提供最新的威胁情报信息，进一步提供 NGTP 方案对 APT 威胁检测的准确性。
- 解决方案技术领先　　组成 NGTP 解决方案的各个模块技术先进。TAC 产品，是国内最早推向市场的 APT 检测设备，经过几年的不断优化，功能和性能得到极大提高，尤其是获得专利技术的静态 Shellcode 检测技术和虚拟执行检测技术，更是为 APT 威胁检测的准确性提供强力支撑。绿盟 NIPS 产品也是久负盛誉，不仅在国内市场上遥遥领先，还多次于国际权威检测机构得到认可。绿盟安全威胁信誉系统，提供最新最全的安全信誉，让 NGTP 方案发挥最大效能。

.

威胁情报

SECURITY

从目前此次攻击及各方面应对情况来看，对于一些高级攻击形式，关键在于尽可能快的了解到相关的情报，以便尽可能快的启动应急响应机制。这无论对于解决木马或者 APT 攻击来说都是重要的手段之一，威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报，并持续对对匿名者攻击事件进行关注，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索绿盟科技联系我们，欢迎您的垂询!

关于绿盟科技

NSFOCUS

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。